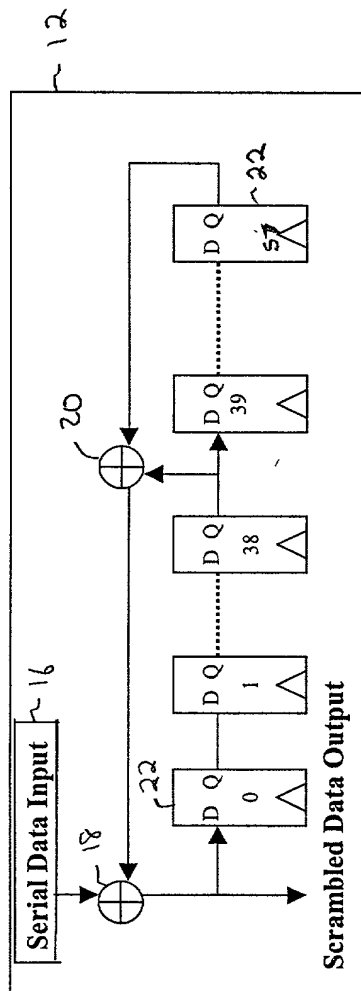


Scrambler Polynomial $1 + X(39) + X(58)$



De-Scrambler Polynomial $1 + X(39) + X(58)$

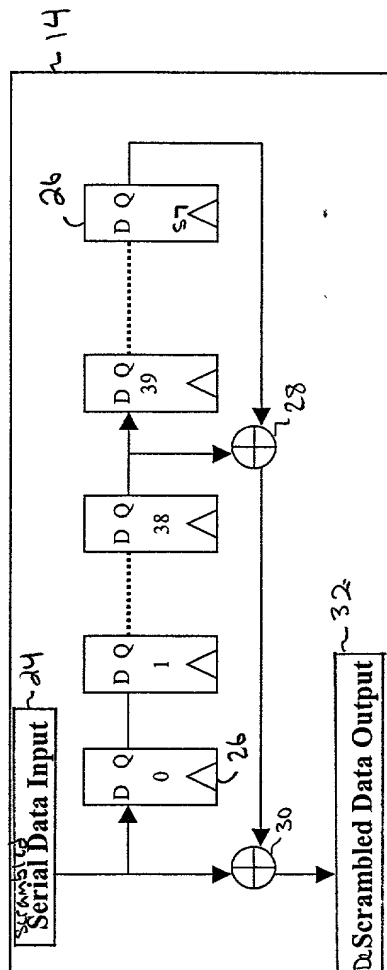


FIG. 1
(PRIOR ART)

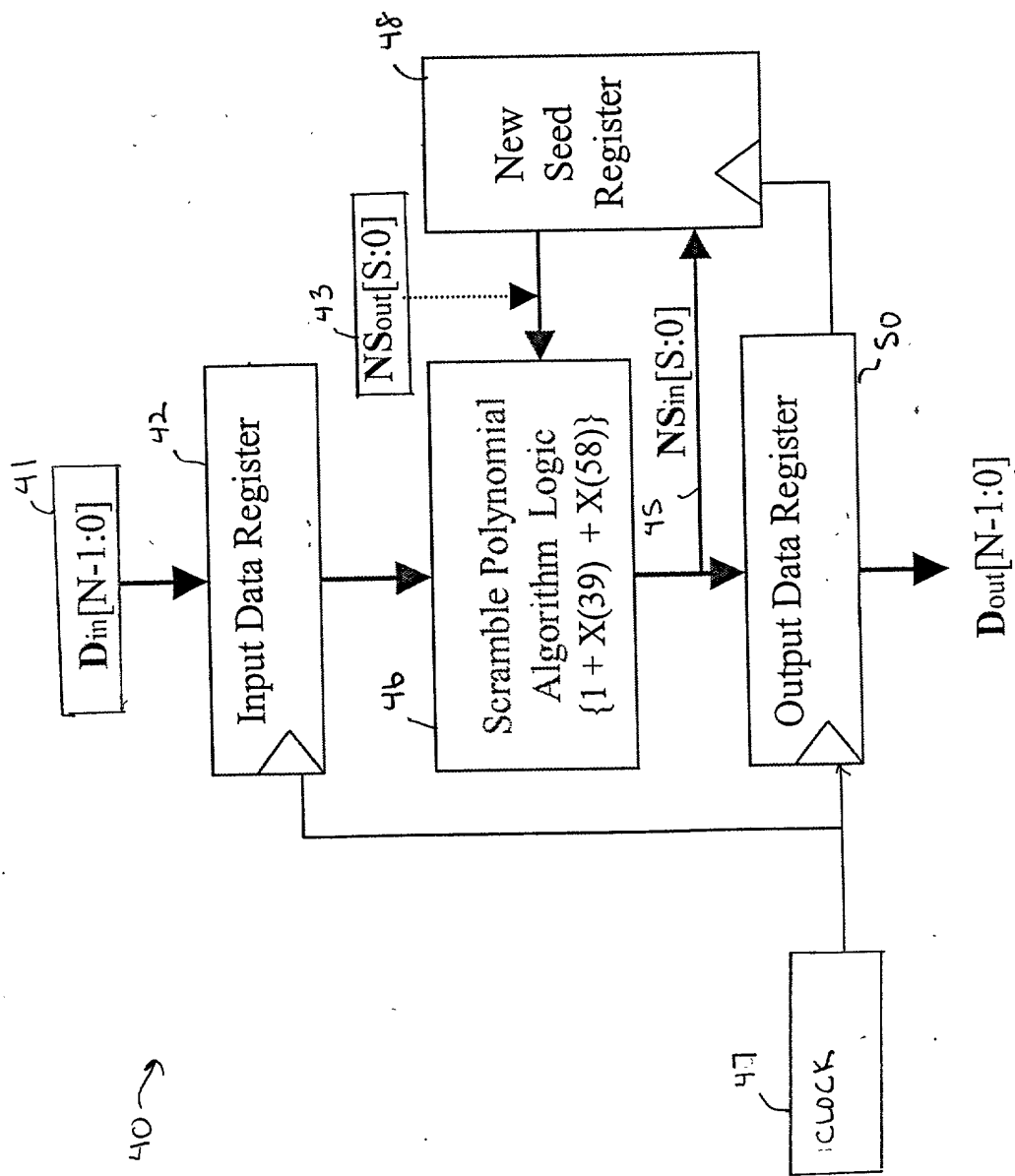


FIG. 2

New Seeds

Ignored
ignored
ignored
ignored
ignored
ignored

Dout(6) => NS'(57);
Dout(7) => NS'(56);
Dout(8) => NS'(55);
Dout(9) => NS'(54);
Dout(10) => NS'(53);
Dout(11) => NS'(52);
Dout(12) => NS'(51);
Dout(13) => NS'(50);
Dout(14) => NS'(49);
Dout(15) => NS'(48);
Dout(16) => NS'(47);
Dout(17) => NS'(46);
Dout(18) => NS'(45);
Dout(19) => NS'(44);
Dout(20) => NS'(43);
Dout(21) => NS'(42);
Dout(22) => NS'(41);
Dout(23) => NS'(40);
Dout(24) => NS'(39);
Dout(25) => NS'(38);
Dout(26) => NS'(37);
Dout(27) => NS'(36);
Dout(28) => NS'(35);
Dout(29) => NS'(34);
Dout(30) => NS'(33);
Dout(31) => NS'(32);
Dout(32) => NS'(31);
Dout(33) => NS'(30);
Dout(34) => NS'(29);
Dout(35) => NS'(28);
Dout(36) => NS'(27);
Dout(37) => NS'(26);
Dout(38) => NS'(25);

Dout(39) => NS'(24);
Dout(40) => NS'(23);
Dout(41) => NS'(22);
Dout(42) => NS'(21);
Dout(43) => NS'(20);
Dout(44) => NS'(19);
Dout(45) => NS'(18);
Dout(46) => NS'(17);
Dout(47) => NS'(16);
Dout(48) => NS'(15);
Dout(49) => NS'(14);
Dout(50) => NS'(13);
Dout(51) => NS'(12);

FIG. 3

Dout(52) => NS'(11);
Dout(53) => NS'(10);
Dout(54) => NS'(9);
Dout(55) => NS'(8);
Dout(56) => NS'(7);
Dout(57) => NS'(6);

Dout(58) => NS'(5);
Dout(59) => NS'(4);
Dout(60) => NS'(3);
Dout(61) => NS'(2);
Dout(62) => NS'(1);
Dout(63) => NS'(0);

FIG. 3

Scrambler Polynomial of $1 + X(39) + X(58)$

```

Dout[0:38] = NS[38:0] ^ NS[57:19] ^ Din[0:38];
Dout(0) = NS(38) ^ NS(57) ^ Din(0);
Dout(1) = NS(37) ^ NS(56) ^ Din(1);
Dout(2) = NS(36) ^ NS(55) ^ Din(2);
Dout(3) = NS(35) ^ NS(54) ^ Din(3);
Dout(4) = NS(34) ^ NS(53) ^ Din(4);
Dout(5) = NS(33) ^ NS(52) ^ Din(5);
Dout(6) = NS(32) ^ NS(51) ^ Din(6);
Dout(7) = NS(31) ^ NS(50) ^ Din(7);
Dout(8) = NS(30) ^ NS(49) ^ Din(8);
Dout(9) = NS(29) ^ NS(48) ^ Din(9);
Dout(10) = NS(28) ^ NS(47) ^ Din(10);
Dout(11) = NS(27) ^ NS(46) ^ Din(11);
Dout(12) = NS(26) ^ NS(45) ^ Din(12);
Dout(13) = NS(25) ^ NS(44) ^ Din(13);
Dout(14) = NS(24) ^ NS(43) ^ Din(14);
Dout(15) = NS(23) ^ NS(42) ^ Din(15);
Dout(16) = NS(22) ^ NS(41) ^ Din(16);
Dout(17) = NS(21) ^ NS(40) ^ Din(17);
Dout(18) = NS(20) ^ NS(39) ^ Din(18);
Dout(19) = NS(19) ^ NS(38) ^ Din(19);
Dout(20) = NS(18) ^ NS(37) ^ Din(20);
Dout(21) = NS(17) ^ NS(36) ^ Din(21);
Dout(22) = NS(16) ^ NS(35) ^ Din(22);
Dout(23) = NS(15) ^ NS(34) ^ Din(23);
Dout(24) = NS(14) ^ NS(33) ^ Din(24);
Dout(25) = NS(13) ^ NS(32) ^ Din(25);
Dout(26) = NS(12) ^ NS(31) ^ Din(26);
Dout(27) = NS(11) ^ NS(30) ^ Din(27);
Dout(28) = NS(10) ^ NS(29) ^ Din(28);
Dout(29) = NS(9) ^ NS(28) ^ Din(29);
Dout(30) = NS(8) ^ NS(27) ^ Din(30);
Dout(31) = NS(7) ^ NS(26) ^ Din(31);
Dout(32) = NS(6) ^ NS(25) ^ Din(32);
Dout(33) = NS(5) ^ NS(24) ^ Din(33);
Dout(34) = NS(4) ^ NS(23) ^ Din(34);
Dout(35) = NS(3) ^ NS(22) ^ Din(35);
Dout(36) = NS(2) ^ NS(21) ^ Din(36);
Dout(37) = NS(1) ^ NS(20) ^ Din(37);
Dout(38) = NS(0) ^ NS(19) ^ Din(38);
Dout[39:57] = NS[18:0] ^ NS[38:20] ^ NS[57:39] ^ Din[0:18] ^ Din[39:57];
Dout(39) = NS(18) ^ NS(38) ^ NS(57) ^ Din(0) ^ Din(39);
Dout(40) = NS(17) ^ NS(37) ^ NS(56) ^ Din(1) ^ Din(40);
Dout(41) = NS(16) ^ NS(36) ^ NS(55) ^ Din(2) ^ Din(41);
Dout(42) = NS(15) ^ NS(35) ^ NS(54) ^ Din(3) ^ Din(42);
Dout(43) = NS(14) ^ NS(34) ^ NS(53) ^ Din(4) ^ Din(43);
Dout(44) = NS(13) ^ NS(33) ^ NS(52) ^ Din(5) ^ Din(44);
Dout(45) = NS(12) ^ NS(32) ^ NS(51) ^ Din(6) ^ Din(45);
Dout(46) = NS(11) ^ NS(31) ^ NS(50) ^ Din(7) ^ Din(46);
Dout(47) = NS(10) ^ NS(30) ^ NS(49) ^ Din(8) ^ Din(47);
Dout(48) = NS(9) ^ NS(29) ^ NS(48) ^ Din(9) ^ Din(48);
Dout(49) = NS(8) ^ NS(28) ^ NS(47) ^ Din(10) ^ Din(49);
Dout(50) = NS(7) ^ NS(27) ^ NS(46) ^ Din(11) ^ Din(50);
Dout(51) = NS(6) ^ NS(26) ^ NS(45) ^ Din(12) ^ Din(51);
Dout(52) = NS(5) ^ NS(25) ^ NS(44) ^ Din(13) ^ Din(52);
Dout(53) = NS(4) ^ NS(24) ^ NS(43) ^ Din(14) ^ Din(53);
Dout(54) = NS(3) ^ NS(23) ^ NS(42) ^ Din(15) ^ Din(54);

```

FIG. 4

Dout(55) = NS(2) ^ NS(22) ^ NS(41) ^ Din(16) ^ Din(55);
Dout(56) = NS(1) ^ NS(21) ^ NS(40) ^ Din(17) ^ Din(56);
Dout(57) = NS(0) ^ NS(20) ^ NS(39) ^ Din(18) ^ Din(57);
Dout[58:63] = NS[19:14] ^ NS[57:52] ^ Din[0:5] ^ Din[19:24] ^ Din[58:63];
Dout(58) = NS(19) ^ NS(57) ^ Din(0) ^ Din(19) ^ Din(58);
Dout(59) = NS(18) ^ NS(56) ^ Din(1) ^ Din(20) ^ Din(59);
Dout(60) = NS(17) ^ NS(55) ^ Din(2) ^ Din(21) ^ Din(60);
Dout(61) = NS(16) ^ NS(54) ^ Din(3) ^ Din(22) ^ Din(61);
Dout(62) = NS(15) ^ NS(53) ^ Din(4) ^ Din(23) ^ Din(62);
Dout(63) = NS(14) ^ NS(52) ^ Din(5) ^ Din(24) ^ Din(63);

FIG. 4

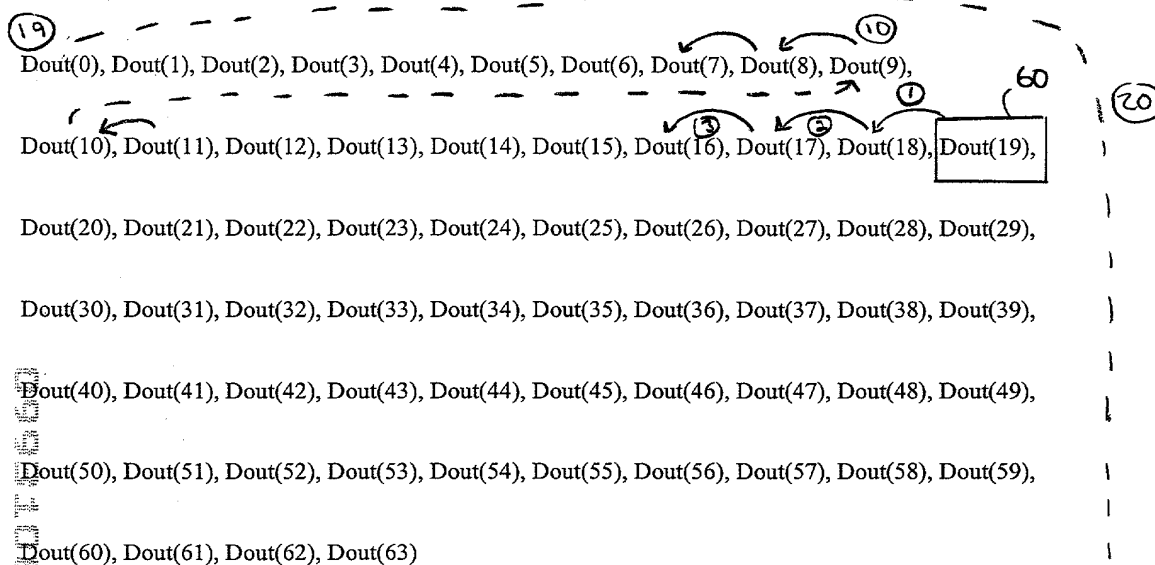
09578801 09072660

SCRAMBLER POLYNOMIAL

$$1 + x^{39} + x^{58}$$

$$\text{Dout}(19) = \text{NS}(19) \wedge \text{NS}(38) \wedge \text{Din}(19)$$

Scrambled Output current clock period (time = t)



(time = t-1)

Previous scrambled output for previous clock period

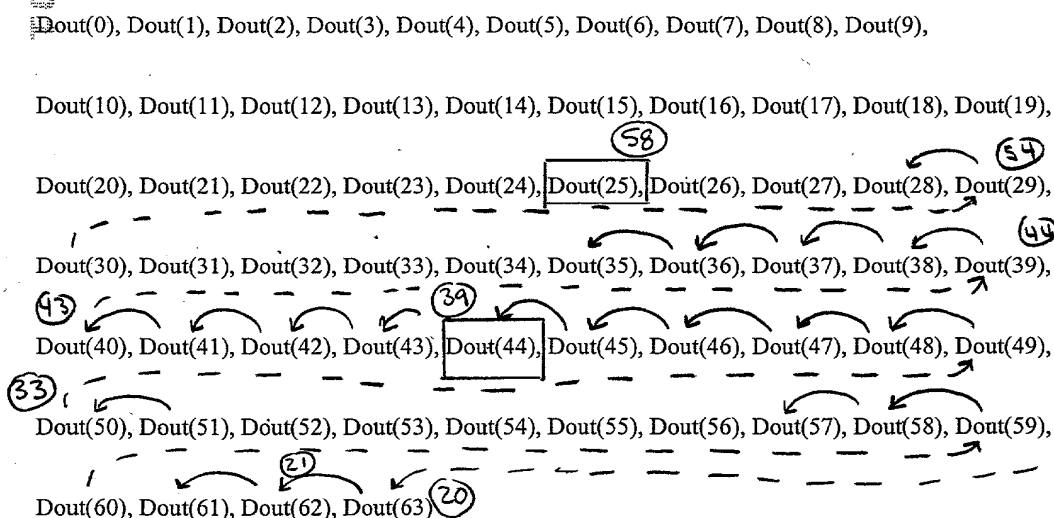


FIG 5

Scrambler Polynomial $1+X(39)+X(58)$

$Dout(50)=NS(7)^{NS(27)^{NS(46)^{Din(11)^{Din(50)}}$

Scrambled Output for current clock period (time=t)

$Dout(0), Dout(1), Dout(2), Dout(3), Dout(4), Dout(5), Dout(6), Dout(7), Dout(8), Dout(9),$
 $Dout(10), \boxed{Dout(11)}, Dout(12), Dout(13), Dout(14), Dout(15), Dout(16), Dout(17), Dout(18), Dout(19),$
 $Dout(20), Dout(21), Dout(22), Dout(23), Dout(24), Dout(25), Dout(26), Dout(27), Dout(28), Dout(29),$
 $Dout(30), Dout(31), Dout(32), Dout(33), Dout(34), Dout(35), Dout(36), Dout(37), Dout(38), Dout(39),$
 $Dout(40), Dout(41), Dout(42), Dout(43), Dout(44), Dout(45), Dout(46), Dout(47), Dout(48), Dout(49),$
 $\boxed{Dout(50)}, Dout(51), Dout(52), Dout(53), Dout(54), Dout(55), Dout(56), Dout(57), Dout(58), Dout(59),$
 $Dout(60), Dout(61), Dout(62), Dout(63)$

Scrambled Output for previous clock period (time=t-1)

$Dout(0), Dout(1), Dout(2), Dout(3), Dout(4), Dout(5), Dout(6), Dout(7), Dout(8), Dout(9),$
 $Dout(10), Dout(11), Dout(12), Dout(13), Dout(14), Dout(15), Dout(16), Dout(17), Dout(18), Dout(19),$
 $Dout(20), Dout(21), Dout(22), Dout(23), Dout(24), Dout(25), Dout(26), Dout(27), Dout(28), Dout(29),$
 $Dout(30), Dout(31), Dout(32), Dout(33), Dout(34), Dout(35), Dout(36), Dout(37), Dout(38), Dout(39),$
 $Dout(40), Dout(41), Dout(42), Dout(43), Dout(44), Dout(45), Dout(46), Dout(47), Dout(48), Dout(49),$
 $Dout(50), Dout(51), Dout(52), Dout(53), Dout(54), Dout(55), \boxed{Dout(56)}, Dout(57), Dout(58), Dout(59),$
 $Dout(60), Dout(61), Dout(62), Dout(63)$

FIG. 6

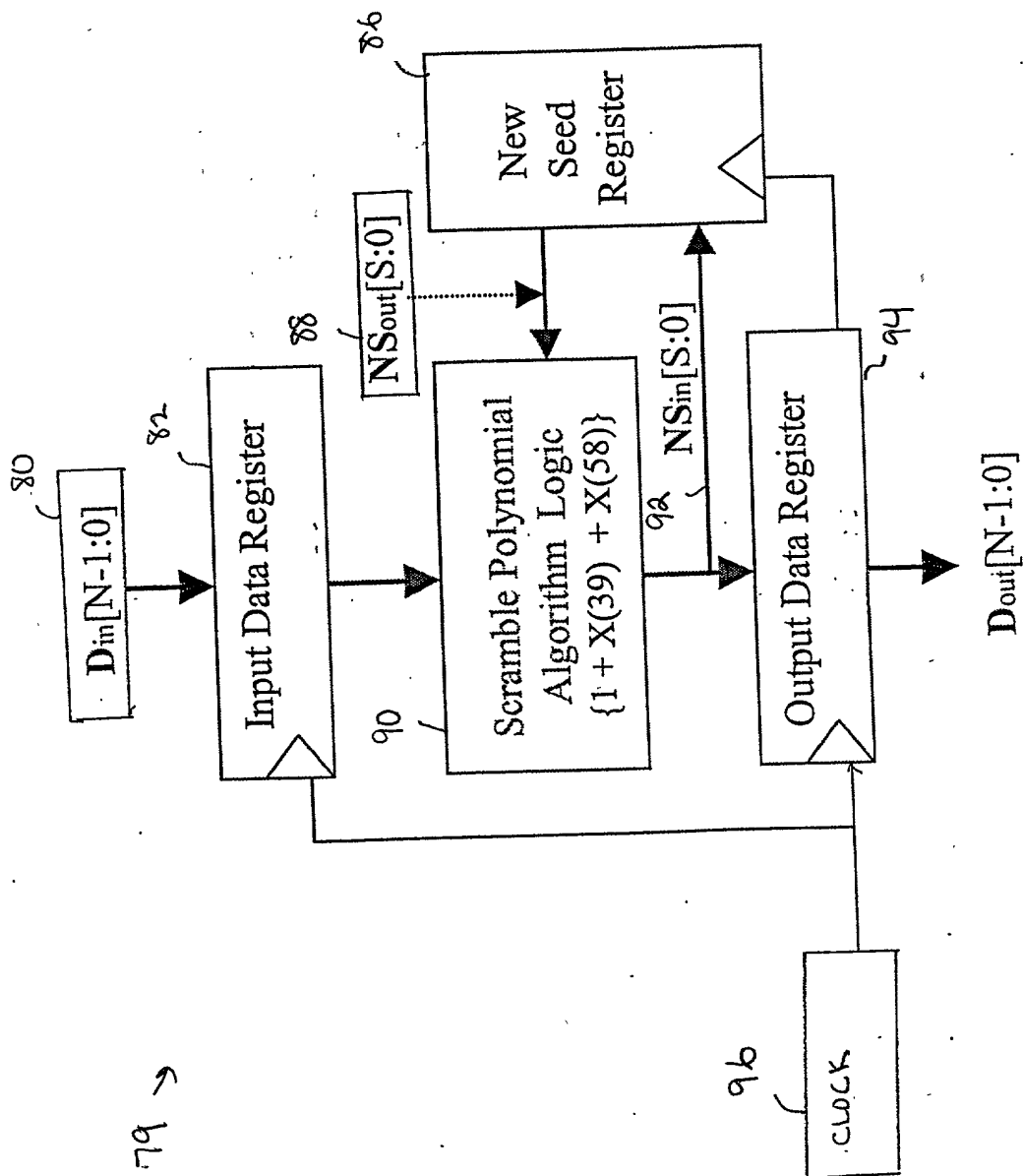


FIG. 7

99

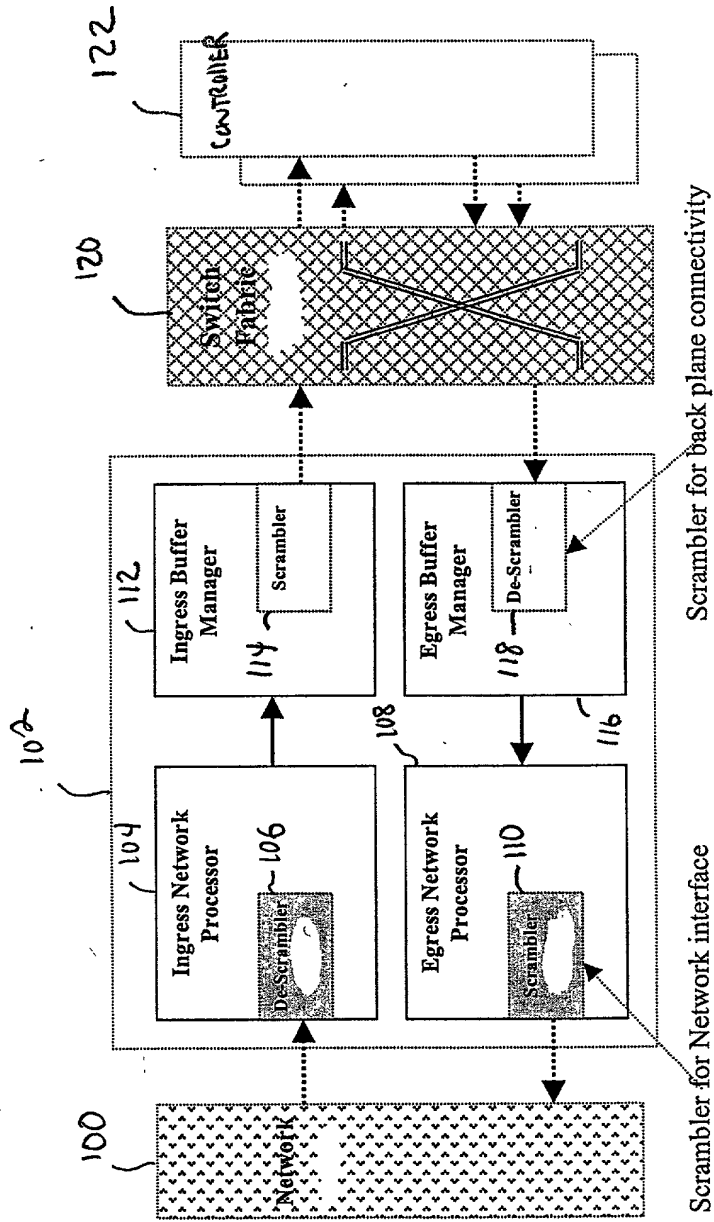


FIG. 8